(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 July 2002 (11.07.2002)

PCT

(10) International Publication Number
WO 02/054341 A1

(51) International Patent Classification[7]: G06K 9/00, G06F 17/60, 11/30, 12/14, H04L 9/00, 9/32

(21) International Application Number: PCT/US02/00637

(22) International Filing Date: 8 January 2002 (08.01.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/260,195 8 January 2001 (08.01.2001) US

(71) Applicant *(for all designated States except US)*: **STEFAAN DE SCHRIJVER, INCORPORATED** [US/US]; 952 Beacon Street, Newton, MA 02459 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **LENT, Michelle, A.** [US/US]; 1730 La Loma Avenue, Berkeley, CA 94709 (US).

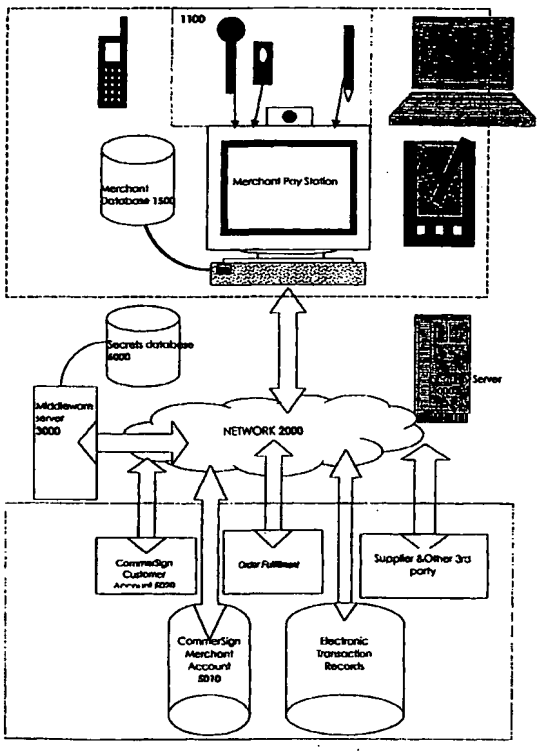
(74) Agents: **LOREN, Ralph, A.** et al.; Lahive & Cockfield, LLP, 28 State Street, Boston, MA 02109 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: COMMERSIGN: SYSTEMS AND METHODS FOR SECURE ELECTRONIC BUSINESS TRANSACTIONS



(57) Abstract: The invention provides a transaction system (1000, 1100, 1500, 2000, 3000, 4000, 5000, 5010, 5020, 6000) wherein, when an entity (person, company, computer program), transaction, document or thing needs to be authenticated, information regarding one or more of the parties or items (such as electronic records) involved is associated with biometric data of at least one of the parties. The electronic records are hashed with a session key. Biometric data regarding at least one of the parties authorizing the transaction are measured with biometric means (such as signature dynamics). The biometric means I 100 have a unique identification key (ID). The ID and the session key are used to create a transaction key. The transaction key is used to encrypt the HASH and the dynamic biometric data of the authorizing individual or individuals. The biometric data of the individuals are used to authenticate the identity of the individual.

WO 02/054341 A1

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

CommerSign: SYSTEMS AND METHODS FOR SECURE ELECTRONIC BUSINESS TRANSACTIONS

BACKGROUND OF THE INVENTION

1. Field of The Invention

The invention relates to systems and methods for allowing consumers, businesses and other entities to place orders, deliver goods and perform payments or authorize credits employing a biometric device as identifier.

The present invention relates generally to systems that secure privacy and confidentiality of the above transactions and, more particularly, concerns a method and apparatus for authenticating documents, records and objects as well as individuals who are involved with or responsible for said transactions.

2. Background of The Invention

There are situations that require secure transactions. Security is founded on the combination of authentication, entitlement, integrity, non-repudiation and confidentiality of transactions and of the associated documents and objects. Authentication verifies the identity of entities; entitlement verifies the right of an entity to execute a transaction; confidentiality protects the transaction and all its linkage from publicity; integrity ensures that any information or documentation regarding the transaction remains constant and unchanged; non-repudiation provides legal proof that the transaction occurred.

For example checks, stock certificates, and bonds are subject to theft. Electronic payment transfers are subject to fraud. From the time a document is issued, the information contained on it, or the name of the recipient could be changed. False documents can be issued with forged images of signatures. Similarly, passports, pay checks, motor vehicle registrations, diplomas, food stamps, wager receipts, medical prescriptions, or birth certificates and other official documents are subject to forgery, fraudulent modification or use by an unintended recipient. To counter this, special forms, official stamps and seals, and special authentication procedures have been

utilized to assure the authenticity of such documents. Medical, legal and personnel records, and all types of information in storage media are also subject to unauthorized access. Pin-codes, passwords, encrypting and hashing of such records are used in the art to thwart unauthorized access and tampering. ecently it has come to light that fraud with promotional coupons is widespread, and was used to finance terrorist networks.

Computers and computer networks used to conduct transactions and document processing, allow early detection of certain types of fraud. However, eliminating the human connection makes verification of the identity of transacting entities essential, since the trust factor that exists between humans who know each other has been eliminated. Therefore the need remains for business transaction, document processing, and access systems which can secure a transaction.

In the context of the present document, "access systems" mean systems which access networks or media which contain, store, process, transmit, transport or carry physical, or electronic analog or digital data, messages, text, FAX, audio, video, drawings, images, photo, electronic and physical mail, safe boxes, biometric information and the like. In the context of the present document, "transaction system" means all such transaction, payment, document processing, access systems, and trusted third party systems, including ones not related to business use, such as passport authentication systems.

Today applications that allow order placement, fulfillment and payment by means of credit cards are common, whether at point of sales, or over the Internet for so-called electronic-commerce. These applications are well known in the art. They require the users to identify themselves by means of a pin code and a name, with additional information such as date of birth, mother's maiden name, (part of) social security number, expiration date, last transaction amounts etc...

Service providers keep this information together with the pre-registered templates, which include address and other personal data, and with the history of the transactions. These "secrets" often are shared by the service providers, such as banks, by depositing them with third parties such as credit bureaus like Equifax. These measures, while widely used with private networks, are not very adequate for use with open networks such as Internet, where identity easily can be stolen.

The security problems described above have been acerbated by the advent of electronic business conducted over the Internet. To some extent, systems involving Public Key Infrastructures have been able to solve some of the security issues. However they require the deployment of novel transactions systems, and, above all, they use methods and apparatus that do not permit the linkage of individuals to the transactions that they execute. Therefore these PKI systems do not provide proof positive of an individual's participation in a transaction. The overwhelming majority of currently deployed computer networks are private closed networks. PKI works well with open networks. For closed networks other facilities are required.

Therefore there is a need in the art for a transaction system that secures the interests of all parties to multi-party transactions whether the parties are present or absent to a transaction, whether the transaction occurs over public or private, open or closed systems. There is a need in the art for systems that undeniably link individuals with the transactions that they are involved with. There is also a need in the art to do this at as low a possible cost. Therefore there is a need in the art to provide authentication of individuals without the usage of credit cards or smartcards or magnetic stripe cards. The means to do so require biometrics.

SUMMARY OF THE INVENTION

It is the object of the present invention to provide apparatus and methods that allow electronic commerce fulfillment and payment, through credit, debit or electronic cash transactions, without the usage of cards or other such tokens used in the identification of individuals. The present invention is directed to a centralized transaction system, which avoids the shortcomings of such systems currently used in the art.

The invention includes the following apparatus:

A plurality of client devices including a computer and a means of network communication (**1000**: cash register or other point of sales terminal, a PDA, a home computer, a television with a set-top box , or a (wireless) telephone).

A plurality of biometric means (**1100**: smartpen, fingerprint device, camera, microphone for voice recognition, etc.) that can be used alone or conjointly for biometric measurements.

A plurality of electronic commerce application servers **5000**(for credit evaluation, for order transaction, for payment transaction, for order fulfillment, etc...).

A plurality of security servers **4000** (for biometric authentication modules including registration and verification, for secure key management and encryption, for validation of biometric devices, for template databases, etc....) providing security of data, confidentiality of protocols, privacy of profiles and non- repudiation of transactions.

A network infrastructure **2000** including LAN/ WAN/ MAN/ PAN/ VPN/ Intranet/ Internet wired or wireless networks for digital data transfers.

A plurality of software agents **3000** including user interfaces, secure socket layers, network management, content management, "middle ware", database management, error recovery and exception handling, all known in the art.

A plurality of profiles that constitute databases **6000** regarding the buying, credit, and payment habits of buyers, whether consumers or professional purchasers for companies. Such profiles are treated in the art as shared secrets.

The present invention provides processes that vary only slightly whether the parties are present to the transaction (for instance a buyer visiting a merchant's store), or absent (such as when purchasing through electronic catalogs, whether from computers, televisions, automatic teller machines, or telephones, wireless or wired). The business process for merchants in stores is described hereafter as an example. Alternative implementations are easily derived. The business process can be used for the sale of hard or soft goods, as well as for services.

The invention provides a transaction system wherein, when an entity (person, company, computer program), transaction, document or thing needs to be authenticated, information regarding one or more of the parties or items (such as electronic records) involved is associated with biometric data of at least one of the parties. The electronic records are hashed with a session key. The hash is time stamped. Biometric data regarding at least one of the parties authorizing the transaction are measured with biometric means (such as signature dynamics). The biometric means **1100** have a

unique identification key (ID). The ID and the session key are used to create a transaction key. The transaction key is used to encrypt the HASH and the dynamic biometric data of the authorizing individual or individuals. The biometric data of the individuals are used to authenticate the identity of the individual. This results in a proof of signature verification (PSV). The HASH, the PSV, the transaction key, and the time stamp are used to maintain the integrity and confidentiality of the transaction and the items and entities related to it.

They are stored in a shared secrets database 6000 and can be used to decrypt and decode the HASH to restore the original electronic record of the transaction. The electronic information must then match the record printed on or otherwise attached to any physical items.

DRAWING: An illustration of the CommerSign Transaction System

The following drawing illustrates some of the components that constitute a possible embodiment of the CommerSign transaction system.

DESCRIPTION OF AN ILLUSTRATIVE EMBODIMENT

The foregoing brief description as well as further objects, features, and advantages of the present invention will be understood more completely from the following detailed description of the illustrative embodiments of the invention, with reference to the accompanying drawing.

In accordance with an embodiment of the present invention, a merchant opens a CommerSign merchant account **5010** or a plurality of such accounts, with a bank or other financial institution. The bank creates a merchant profile. Such a profile may contain a plurality of suspense accounts automatic billing and payment links to the suppliers of the merchant. It also may contain automatic insurance against credit risks, fraud, and other such payment exceptions. The profile may contain credentialing and entitlement information regarding officers of the merchant. In anyway such a profile maintains a record of the commercial behavior of the merchant. The bank may use known credentialing systems to authorize certain credits to the merchant and or the supplier. The bank may aggregate the payments and billings and clear the balances of

the accounts on a periodic (daily, weekly) basis, thus providing payment facilities to the merchants and the suppliers, through the CommerSign system. In such a case the Bank uses the CommerSign system in a recursive way. The bank may aggregate the CommerSign transaction system with other services it provides the merchant, such as insurance, employee benefits, investment, mortgage, savings accounts.

The bank provides the entire infrastructure for the CommerSign business system, or links the merchant's system to the CommerSign business system, in either case the bank provides a Virtual Private Network **2000** and all the necessary apparatus to be used during the transaction.

The merchant through known means (such as coupons, loyalty schemes, gifts) in cooperation with the bank convinces the customer (consumer or corporate buyer) to open a CommerSign customer **5020** (personal, family or corporate) account. To that purpose customers register certain personal, family or corporate information as the case may be, including entitlements to the usage of the CommerSign account and including personal biometric information such as facial, finger, voice, or signature dynamics. The bank creates a customer profile including all the biometrics it registered. The bank can use known shared secret services to decide on the amount of credit to authorize for each account. Or the bank can link the CommerSign account to existing accounts, such as checking accounts, thus creating a debit facility. Either way the bank creates a payment facility from the customer to the merchant. The bank may aggregate the CommerSign account with other accounts of the customer, such as savings, mortgage, investments, insurance. In this way the bank may use the CommerSign account in other circumstances than the retail purchases.

All profiles regarding people, whether officers of the merchant or customers or their family members must contain a record of information such as follows:

- An assumed identity including: name, address, telephone number, fax number, e-mail address, relation to the account holder, employer identification, date of birth, social security number, and the like,
- Static Biometric Data including one or a plurality of static biometric reference templates of fingerprint minutia, iris pictures, face patterns, pen signature image (from static reconstruction with tablets or form reconstruction through force dynamics) and the like,

- Dynamic Biometric Data including one or a plurality of biometric reference templates: Pen signature dynamics, seal/stamp dynamics (such as three dimensional forces on the pen tip, three dimensional angles of the pen with a magnetic field, two dimensional angles of the pen with a gravitational field, forces on the body of the pen, accelerations of the pen body, pen strokes, motion in the air, pen-up/pen-down status, time dependencies of the foregoing leading to frequency measurements, as well as amplitude measurements), voice fenones including time dependencies of frequencies and amplitudes,

- Historic Behavior Data: of the biometric device as well as of the persons: where do they usually operate, what do they usually perform or purchase and the like

Entitlements: determine the kind of transactions, the kind of goods, the level of credits, the kind of accesses a person in the CommerSign system can have

Links for Aggregation: what accounts provide, receive, or share information with the CommerSign accounts, and how to securely transfer the information.

Further, for the case where customers visit a store and are present when the transaction occurs, the following embodiment of the business process and transaction system can be envisioned.

A customer enters a store and collects the goods to be purchased from the shelves.

The goods are either property of the merchant or of the supplier, in case the merchant rents shelf space to the supplier and sells the goods on a consignment basis.

When the customer presents the goods at the payment counter the goods, the customer, the transaction, and a payment slip must be identified. The goods are identified by means of a scanning device connected to the cash register. The customer is identified by providing his/her name through biometric means, such as voice or face recognition, or through an identification document such as a driver's license, social security card, photo ID or any other means known in the art. The Biometric Stylus is activated by the pay station. The Biometric Stylus sets up a transaction session with the BiSS. An unique Session Key is created by the Biometric Security System (BiSS). An electronic transaction record is created, then displayed on the pay station and printed on the payment slip together with its time stamp as originated in the BiSS. The session key is used to hash the electronic transaction record (ETR). The HASH is also printed on

the associated payment slip. When the customer signs the payment slip with a biometric stylus the latter produces biometric signature dynamics (BSD) and preferably a timestamp for the BSD. The biometric stylus uses its unique stylusID together with the unique session key to create a unique transaction key. The BiSS, which created the session key and knows the stylus ID, uses the unique transaction key to encrypt the hash together with the BSD into a secure record while it is transmitted from the pay station to the biometric authentication module (BAM). The customer's ID was transmitted in clear and used to retrieve the customer's biometric template from the shared secrets database. The BAM now produces an OK or a NOK message. This message is encrypted together with a proof of signature verification (PSV) with the same transaction key and returned to the biometric stylus and subsequently to the pay-station. The shared secrets database is now updated with the Hash, the time stamp of the PSV issued, the PSV, NOK or OK result, and the transaction key.

The session key is a unique random number generated by the BiSS, independent of any transacting party. That code is used to hash the information regarding the electronic transaction or ETR. No information regarding the transacting parties is used to code information regarding the transaction. The Stylus ID is unique to the device used to produce the biometric signature dynamics. In itself it does not contain any information regarding the transacting parties. The Stylus ID is combined together with the session key to create a unique transaction key. The transaction key is used to encrypt the combination of the hash and the BSD. As a consequence, the confidentiality of the customer is maintained vis-à-vis the merchant, since only the trusted third party, in this case the bank, has access to the shared secrets database. Only the BSD of the customer is used for authentication purposes since the entire transaction system operates as a private or as a virtual private network, whereby the second transacting party is always the merchant, and does not need authentication, since the merchant is the operator or virtual operator of the transaction system. The hash is not used to authenticate the transaction, merely to maintain its integrity. The PSV is used to authenticate the transaction.

The result of the authentication is either an OK or a NOK.

If the result of the authentication is an OK, the bank verifies the level of entitlement of the individual. This results in an OK or a NOK. The shared secret

database is updated with the result and with the timestamp of the result. The payment is charged to the customer account. The merchant's suspense account is credited. The entitlement OK together with the authentication OK and the proof of signature verification are encrypted with the transaction key and returned to the biometric device at the pay station. The biometric device instructs the pay station to update the merchant's information system and the ETR and to this end transmits in clear the timestamp of the creation of the PSV to the pay-station.

If the result of the entitlement verification is NOK, an Entitlement Exception Handling (EHE) message is transmitted to the pay station. The merchant handles this according to known procedures. A record is made in the merchant's information system as well as in the shared secret database.

If the result of the authentication is a NOK, an Authentication Exception Handling (AHE) message is transmitted to the pay station. The merchant handles this according to known procedures. A record is made in the merchant's information system as well as in the shared secret database.

The customer now receives the goods and leaves the premises, or leaves the premises without the goods, as the case may be.

At the end of the agreed period the bank clears all the payments in the merchant's suspense account and credits the merchants current account.

If the embodiment includes the recursive capability the payments from and to the merchant's suppliers are automatically balanced out. The merchant's information system receives a report and can be updated according to established protocols. Anyway the merchant's profile is updated by the bank.

In case of dispute, for instance when the customer returns the goods, the ID of the customer, the HASH and the timestamp of the transaction are submitted to the BiSS that recreates the ETR from the information in the shared secrets database. To the extent that nobody tampered with the records, the ETR, the printed pay slip and the reconstructed ETR will contain the same information. In order to allow the reconstruction of the ETR from the HASH, the customer must sign an authorization transaction, which has a protocol similar to the purchase transaction. Thus reconstruction of the HASH can only occur if the original customer comes and signs for the reconstruction request, thus guaranteeing the confidentiality of the transaction.

Since the bank has the ETR only in HASH form, it cannot use the information of the ETR without the explicit authorization of the customer. The bank can only use its shared secrets file for statistical and credentialing information.

As opposed to other known secure transaction systems, customers are not required to remember PIN codes, since their biometrics are used to the purpose of identifying them.

Although preferred embodiments of the invention have been disclosed for illustrative purposes, those skilled in the art will appreciate that many additions, modifications, and substitutions are possible without departing from the scope or spirit of the invention as described above.

What is claimed is:

1. A centralized system for electronic commerce.

2. A method, using centralized electronic commerce systems according to claim 1.

3. A method, according to claim 2, whereby the system of claim 1 provides secure electronic commerce.

4. A method, according to claim 2, whereby the system of claim 1 provides privacy in the conduct of the conduct of electronic commerce.

5. A method, according to claim 2, providing proof positive of an individual's participation in the commercial transactions.

6. A method, according to claim 5, using electronic signatures.

7. A method, according to claim 6, providing electronic signatures without depending on Public Key Infrastructure.

8. A method, according to claim 5, providing proof positive of an individual's participation without the use of magnetic cards, smart cards, pin codes, etc. to provide an identity for the individual.

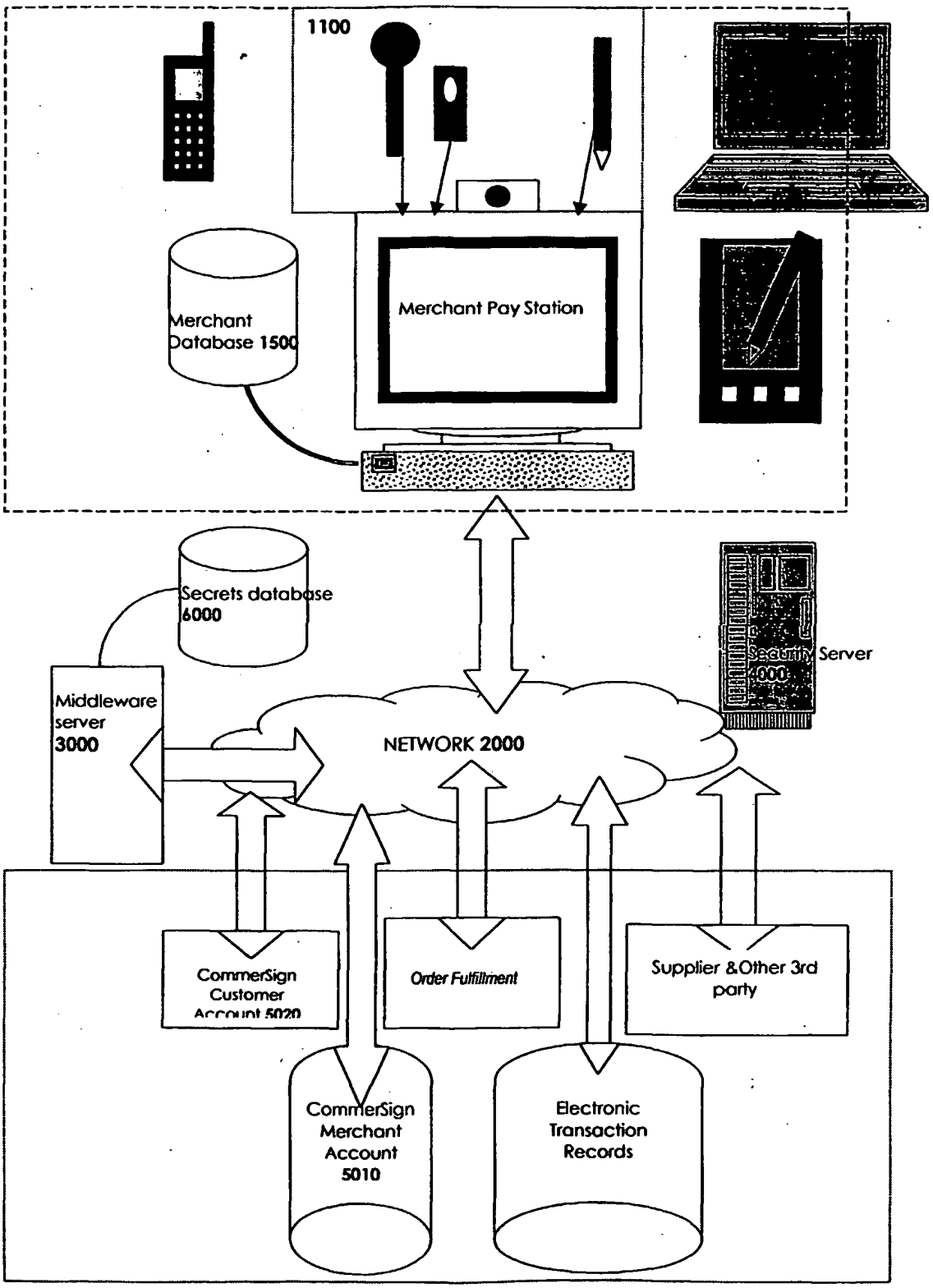
9. A method, according to claim 6, generating and securely storing electronic documents.

10. A method, according to claim 6, recursive use of the method for chain stores.

11. A method, according to claim 10, may involve aggregation of services such as insurance, and other operational financing needs.

12. A method, according to claim 2, enforcing trace-ability of all transactions.

13. A method, according to claim 2, enforcing trace-ability of all documents used in transactions, such as coupons.


1100
Merchant Database 1500
Merchant Pay Station
Secrets database 6000
Middleware server 3000
NETWORK 2000
Security Server 4000
CommerSign Customer Account 5020
Order Fulfillment
Supplier &Other 3rd party
CommerSign Merchant Account 5010
Electronic Transaction Records

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US02/00637

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06K 9/00; G06F 17/60,11/30,12/14; H04L 9/00,9/32
US CL : 382/115; 705/14; 713/200

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 382/115 - 127; 705/64 - 75; 713/186, 200; 705/14-16

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EAST, NPL - IEEEXplore, PROquest; Google

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 5,838,812 A (Pare, Jr. et al) 17 November 1998 (17.11.1998), column 11, lines 28-45; column 28, lines 2-12; column 7, lines 51-56; column 13, lines 8-67; column 14, lines 1-9; column 11, lines 4-16; column 12, lines 18-23; column 6, lines 59-67; column 7, lines 1-6; column 31, lines 16-31; column 31, lines 32-63; column 43, lines 63-65; column 73, lines 49-67; column 12, lines 30-40; column 27, lines 9-18; column 31, lines 16-31; column 7, lines 42-61	1-5, 8, 12 --- 6-7,9-11,13
Y	US 6,035,280 A (Christensen) 07 March 2000 (7.3.2000), column 7, lines 42-61	13
Y	Norton, IBIA (International Biometric Industry Ass.) June 2000 release, page 4	6-7,9-11

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 May 2002 (14.05.2002)	10 JUN 2002
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Gail O Hayes for James R. Matthews Telephone No. 703-306-4153

Form PCT/ISA/210 (second sheet) (July 1998)